A Comparison of the Proof of Work and Proof of Stake Consensus Mechanism

Ádám Blázsek
University College of Northern Denmark
Software Development (PSU0219)
12 April 2019
1062084@ucn.dk

Abstract: Bitcoin pioneered peer to peer transactions back in 2009, by circumventing the middle man (such as banks) it was and still is a futuristic vision for decentralized settlements where anyone can transact with anyone. With the popularity boom however, we have discovered many downsides to the fundamental way transactions are processed. While the interaction does happen, it happens at a rate which modern individuals would view as archaic. Since then, many visionaries have tried to improve upon the original idea to make the speeds viable. This paper will compare the main rival to the Proof of Work consensus mechanism used in Bitcoin with its main rival, Proof of Stake which is increasing in popularity day by day and show why the use of miners in Proof of Work is actually harming rather than aiding the vision by slowing down the transactions and ultimately making the network centralized. The comparison will show how Proof of Work is suffering when talking about scalability while Proof of Stake thrives when expanding the network with a large number of users.

Keywords: Proof of Work, Proof of Stake, Bitcoin, XRP, scalability, blockchain, consensus, comparison, transaction, ledger, decentralization, peer to peer

Preface

Before diving into the investigation, I would like to thank my a few of my colleagues who offered help in the creation and finalization of this research paper.

Finn Ebertsen Nordbjerg for giving feedback on my initial questions, Ralfs Zangis Andrei-Eugen Birta and Michael Zdravkov for their feedback on the final versions of the document.

Introduction

When Bitcoin was created by Satoshi Nakamoto it was intended to be a decentralized network where peer-to-peer transactions would be conducted without the need of an intermediary entity. [1] With the network growing in size it has soon been discovered that the speed of the network is too slow for the needs of today's users.

We will compare the original consensus mechanism used by Bitcoin called Proof of Work against the current most popular alternative called Proof of Stake used by the coin called XRP to see if the original idea could be improved upon to the point where adaption could be a viable option. The main question we will be looking at is: What is the better applicable consensus mechanism to be used in large scale networks where transactions would be conducted on the blockchain, Proof of Work or Proof of Stake?

To better understand the contents of the paper, we will briefly go through a few key terms and concepts which are going to be used later on.

Permissioned vs Permissionless platforms: Blockchain platforms can be classified into two main types permissionless and permissioned. Open-ended systems such as Bitcoin and XRP are permissionless as they are available for use by anyone and the more participants join the closer it is to true decentralization. Any node can conduct transactions as well as take part in the consensus process to advance the blockchain. Permissioned platforms (or private blockchains) such as Hyperledger Fabric and Multichain are aimed at consortiums where participation is close-ended, meaning joining is only possible by the approval of the owner. While clients are allowed to submit transactions, advancing the blockchain is restricted to a fixed set of peering nodes that are run by consortium members. [2]

Cryptocurrencies: The mentioned digital assets Bitcoin and XRP are cryptocurrencies which are part of the permissionless blockchain platform. They allow for value to be transferred in the form of virtual currencies known as tokens. Transfers happen without the need of an intermediate entity such as a bank or a payment transfer service and can transfer amounts of any size.

Block: A block can be imagined as a bundle of transactions or any other information and is to be filled with a finite amount of them. Only the Genesis block (the first one) does not reference the previous block, all the others do, creating the chain. Each block is timestamped and unmodifiable after it has been finalized (only in specific scenarios can the block be modified).

Proof of Work and Proof of Stake: PoW and PoS are consensus mechanisms for cryptocurrencies, while Proof of Work was the original consensus mechanism, it comes with various drawbacks, which mainly consist of speed and expensive computational requirements. The security network with Proof of Work relies on block mining, where each node in the network is required to handle computationally difficult problems to ensure the validity of the newly mined block. Mining is incentivized with rewards.

In Proof of Stake the expensive computation is replaced by the probability to create a block and receive the associated reward, which is proportional to a user's ownership stake in the system. The users with the highest stake in the system have the highest incentive to maintain a secure network. [3]

The proposed methodology

In this section we will present the idea behind the comparison and how taking well documented historical data is more accurate for determining the efficiency of the consensus models than mimicking the transactions on a smaller scale via a private ledger on a small number of computers.

For representing different consensus mechanisms this paper has chosen one popular coin from each group. For the Proof of Work mechanism Bitcoin will be the chosen coin as it is not only the biggest coin using this approach but the oldest. Although originally used to conduct illegal transactions on the dark web, its currently used all over the internet as an alternative to the standard Euro, USD, JPY and other payment methods.

The coin XRP is going to represent the Proof of Stake consensus as it is currently the most popular and widely used coin of its type. In stark contrast to Bitcoin, it is meant to work with the middle entity by speeding up the transactions between banks, acting as a standard currency when facilitating cross border settlements thus eliminating the need for Nostro and Vostro accounts, and it is currently in live testing phases across the world. [4]

Private ledgers which mimic the functionality of public ones, while fundamentally work the same way, they can never fully replicate the behavior of them. This is due to the size and erratic nature of the cryptocurrency market. Hacks happen constantly, bugs are constantly being discovered and the market is heavily manipulated. [5] This is the perfect environment for stress testing a new technology as the number of users is so vast it could never be replicated on a private ledger within a company. At the time of writing, there are over 2 million unique addresses actively used in the Bitcoin and XRP ledger combined. [6] [7] Also, we can never replicate the irrational behavior of the cryptocurrency market. Transaction volume can rise and fall within minutes and in the case of Proof of Work the mining power varies based on the reward amount, perfect for stress testing. This was most apparent in the late 2017 and early 2018 “gold rush” where both consensus methods were pushed to their absolute limits. Below is a visual representation of the “bull run” and subsequent crash which happened almost immediately. [8]

Figure 1: A visual representation of the cryptocurrency market

Data will be gathered from various cryptocurrency information sites (mentioned in the appendix) run by enthusiasts from all around the world. The time frame for our analysis will be between December 1st of 2017 and Feb 1st of 2018 where the number of users, transactions grew parabolically and the overall behavior of the network was much more erratic in comparison to the overall timeframe. The gathered data from both coins [9], will be visualized by the help of Microsoft Power BI.

Data gathering and results

In this section we will be conducting the comparison between the consensus mechanisms by using the representative coins, mainly focusing on the amount of transactions they can handle in a given moment and how efficient they are when looking at the cost of keeping the network running.

Transaction speed

When talking about transaction speed, we usually take into consideration how many transactions a second a network can handle and how a transaction is handled throughout its duration.

When talking about Proof of Work a transaction must be confirmed for it to be carried out. A confirmation means that the transaction is closer to becoming irreversible, as it is verified and will be included in the block to be mined. A payment with zero confirmations has the possibility to be reversed, thus making the minimum waiting time at roughly 10 minutes. [10] Although in theory a single confirmation is enough to carry out a transaction, the community has agreed that the common practice should be a wait for 6 confirmations as that is probabilistically final. [11] While this is certainly good practice, it means the minimum waiting time is about 50-60 minutes. [12] During the 2 months, Bitcoin had the advantage of being popular and mining was still very profitable, this meant even though the network was heavily under load, new blocks were still found in reasonable time, in some cases under 8 minutes, so high value transactions were carried out in the usual 60-minute time. Although while the block was found in reasonable time, the number of transactions were subpar. As the price of bitcoin started dipping, people immediately wanted to transfer their tokens to exchanges, but the block size stayed the same size, thus taking more time to cover all the needed transactions. The transaction speed for Bitcoin slumped to around 2.5 transactions a second. [13] This number is so low as there is a limit to a block size in the code. Although the size of a block is not permanent and has been increased multiple times throughout its life time, at the peak of the load the size was around a single megabyte which was filled instantly. Increasing the size of the block however comes with its drawbacks in the form of higher transaction fees and an overall slowdown in the network due to the computationally heavier workload as miners need to be incentivized to deal with the higher workloads.

Proof of Stake is much more versatile in this regard, as each participant in the network only needs to choose a set of validators. Validators are servers set up specifically to participate actively in the consensus. This list is called UNL (Unique Node List). Validators each propose a set of transactions to be included in the next version of the ledger and if the validators trust the transaction, it will be added, if not it will be removed. The network will operate flawlessly as long as over 80% of the validators behave as expected, if more than 20% is faulty the network will stop making progress.

With XRP the transaction amount jumps to over 1500 tx/s (transactions a second) and they got fully confirmed in a matter of seconds while settlements happened under 5 seconds. According to historical data XRP had 6 validators running full time which were operated by the company called Ripple. [14]

We can clearly see how the distributed agreement model trumps the adversarial method in both efficiency and speed.

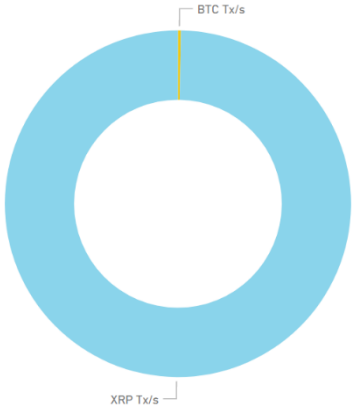

Figure 2: The number of transactions a second visualized. Blue being XRP and Yellow being Bitcoin

Comparing the economic viability

Transaction costs are self-explanatory, they refer to the cost of conducting a transaction. Interestingly both Bitcoin and XRP have dynamic transaction costs (the price of a transaction is linked to the usage of the network) but implemented for completely different reasons. For this section we will take a look at the costs from two different perspectives, one from the user's point of view, looking at the cost of conducting a transaction and the other one is going to be the costs of running the network.

User's point of view

First let's start with the user's point of view. The scenario is a transaction of X amount happening from address A (the user's wallet) to address B (the destination wallet), we will not take into account the speed of the transaction but the cost of conducting the transaction.

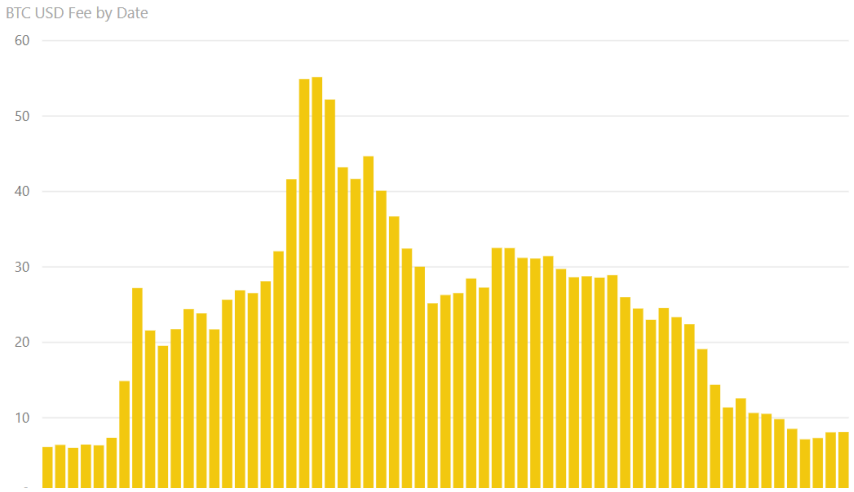

Figure 3: The fee of doing a transaction in USD using Bitcoin between December 2017 and February 2018

When a user conducts a transaction using Bitcoin the fee needed to be paid to the miners are astronomical (over 50 USD on certain days [15]). While relative the price of a single coin at the time of around 20 000 USD it seems reasonable, although the problem is the average person will not actively transact five figure sums thus making the use case for small value transactions irrational as the fee might in some cases be larger than the amount originally meant to be transacted.

Conducting the same transaction with XRP the fee drops dramatically to around 3 cents [16] (3 cents being the worst-case scenario during our period of interest) with a single XRP costing around 3.26 USD. This amount would not be a burden on the user conducting the transaction as it would be nearly identical or lower to what banks charge and could easily be used in the world of online marketplaces.

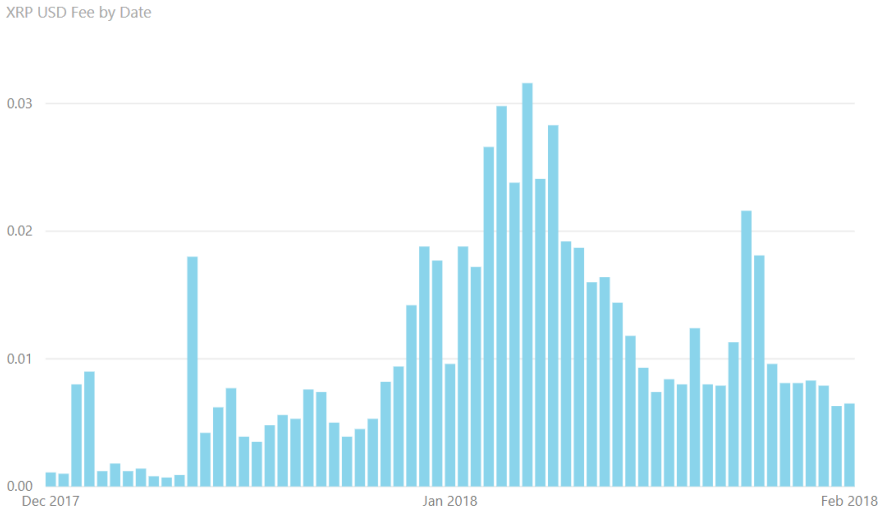

Figure 4: The fee of doing a transaction in USD using XRP between December 2017 and February 2018

Infrastructure's point of view

Now from the infrastructure's standpoint. In this section we will look at the costs accumulated by running the infrastructure.

In this case Proof of Work suffers when considering scalability mainly due to the associated costs of keeping the miners up and running. The problem is the computational heavy load which the miners must handle to keep the transactions happening. Mining is only feasible if the fee for the user is high enough, as that fee is paid to miners as a reward. If the price of bitcoin drops significantly (which it did [17]) the cost of mining the blocks at a profit becomes impossible as it will cost more to carry out the computations (due to hardware costs and electricity consumption) than what the reward for it is, leading the miners working at a loss, leading to many to shut down and slowing down the network.

With the case of Proof of Stake there are no transaction fees required as the computational loads are nonexistent. In the case of XRP, there is a transfer fee of minimum 10 drops (0.00001 XRP) [18] to prevent spamming on the network. The 10 drop fee can be raised if so specified by the sender. The cost in most cases stays the same except for high load scenarios, where the cost is raised by the network to prevent spamming (sending payments just to lower the efficiency of the network). There are no beneficiaries of the fee and it destroys the amount of XRP forever, making XRP scarcer and raising the overall value. Opposed to Proof of Work, the consumption of electricity is also lower by a great margin as a single validator operation costs are roughly the same as a mail server, thus the polluting impact is negligible. [19]

Comparing the two consensus mechanisms in graphs would not make sense as we are comparing thousands of server farms and thousands of home built high performance mining PCs to the equivalent of 6 mail servers. It is however interesting to put into perspective how power hungry bitcoin exactly is. While we don't have exact numbers, we do have very good estimates of what kind of power requirements the network had during the two months. If calculated by the historical hashrate [20] of the network and calculate each machine as using 1500 watts we get the highest recorded energy consumption of about 22.197 TWh which would make the network more power hungry than about 150 countries (using 2016 estimates from the CIA [21]) with the closet comparable one being Ireland with the energy consumption of 23.79 TWh. [22]

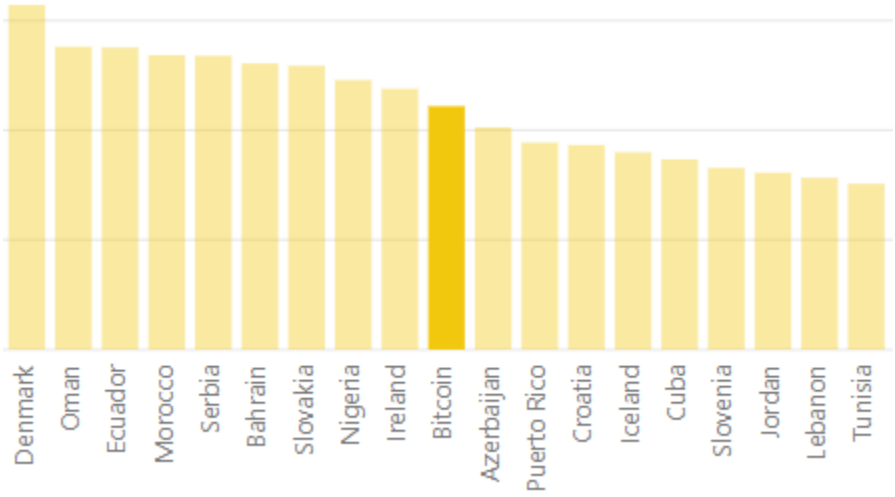

Figure 5: A visual representation of Bitcoin's power hungry nature

Evaluation

In this section we will look at the gathered data and discuss the results.

In this case of Proof of Work versus Proof of Stake where we are comparing Bitcoin and XRP we can clearly see how Proof of Stake is the superior consensus mechanism when looking at the late 2017 early 2018 popularity and price boom. The original use case envisioned for bitcoin where peer-to-peer transactions over the network would circumvent the middle man has certainly been achieved, it is simply not the correct way forward as the two most important things when considering transactions are flawed: price and speed. A possible use case however could be for Bitcoin to become a store of value asset, where the users don't need fast transactions and they would be incentivized to hold the asset rather than trade or transact it (such as gold). Proof of Stake which was built upon its fundamentals has improved the architecture by removing the destructive element: the miners. By removing the party which actively benefits from the raise transaction costs became a far more appropriate option. Not only does it not produce any meaningful environmental damage, it currently outperforms most banks when talking about cross-border transactions. XRP's fee at the current price (at 0.36 USD) is 0.0000127 USD and settlements are finalized within 3.7 seconds.

It is also important not to overlook decentralization when talking about the infrastructure. With mining working on a small scale (as it invites complete strangers to participate in the network and forward its progress) over time it can be subject to centralized control (otherwise known as a 51% attack) and not only block pending transactions but rewrite the history of the ledger to the attacker's pleasure. In Proof of Stake the opposite is true, as a small number of validators can easily be overrun by an attacker, but by increasing the number, it will lead to diversification and a truly democratic network can be achieved.

Finally, the matter of the costs when talking about running the infrastructure is very one sided. While Proof of Work (when looking at Bitcoin) consumes more energy than most smaller countries it has a determinative effect on global warming. Unless the power consumption of computers drops dramatically, let's say to the same point as smartphones in the next few years the use of Proof of Work for conducting transactions is unfeasible next to Proof of Stake which offers better performance at a significantly lower environmental cost.

Discussion

In this section we will discuss the results and see if further investigation is necessary due to uncertainty or limitations.

With the conclusion of Proof of Stake being the superior consensus mechanism in terms of efficiency (financially and technologically), it will be interesting to see how the future of the two approaches play out as Proof of Work is still a more popular option amongst the community and its currently a more popular platform when creating new tokens, but more and more companies are orienting towards the alternative. This is largely trivial as companies want to maximize profits and provide the best possible experience when considering the competition. It is an interesting point as to why startups orientate towards the "less efficient" model. Perhaps the scale of the environment plays a huge role when starting the network. It would be interesting to conduct the same comparison in an environment where the number of users are lower, perhaps Proof of Work edges out in efficiency when the environment has been shrunken. A more accurate comparison could perhaps be conducted via the creation of private ledgers, as the limitations of not being able to replicate millions of users would not be present.

Thanks to the publicity that Blockchain gathered in late 2017 it got enough hyped enough to enter the mainstream in the form of an alternative speculative investment opportunity, but the real use cases for

blockchain based currencies are still to be uncovered, leading companies such as IBM, Oracle and Apple are already investigating this technology and trying their best to uncover its potential by conducting various trials behind closed doors. Although this still being very early in the adoption curve.

Maybe it would be worthwhile revisiting this topic as to where these consensus approaches ended up at in the adoption, to see if maybe Proof of Work does indeed prove to be superior in an environment where Proof of Stake would simply not make sense. Perhaps revisit the same comparison once the new improvements have been implemented for Bitcoin in the form of the Lightning network [23] which promises comparable speeds.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 31 Oct 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed 27 March 2019].

[2] D. A. Baliga, "Understanding Blockchain," April 2017. [Online]. Available: https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf. [Accessed 27 March 2019].

[3] B. Group, "Proof of Stake versus Proof of Work," 15 September 2015. [Online]. Available: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf. [Accessed 3 April 2019].

[4] B. Chase and E. MacBrough, "Analysis of the XRP Ledger Consensus Protocol," 21 February 2018. [Online]. Available: https://arxiv.org/pdf/1802.07242.pdf. [Accessed 27 March 2019].

[5] "www.thenewpaper.io," [Online]. Available: https://www.thenewpaper.io/category/cryptocurrency/. [Accessed 8 April 2019].

[6] "XRP Stats," WieteseWind, [Online]. Available: https://ledger.exposed/rich-stats. [Accessed 10 April 2019].

[7] "blockchain.com," BLOCKCHAIN LUXEMBOURG S.A., [Online]. Available: https://www.blockchain.com/en/charts/n-unique-addresses. [Accessed 10 April 2019].

[8] "nordic.businessinsider.com," Insider Inc / Bonnier Business Media Sweden AB, 02 February 2018. [Online]. Available: https://nordic.businessinsider.com/bitcoin-the-mother-of-all-bubbles-is-now-crashing-2018-2?r=US&IR=T. [Accessed 28 March 2019].

[9] "coingecko.com," [Online]. Available: https://www.coingecko.com/en. [Accessed 28 March 2019].

[10] "buybitcoinworldwide.com," [Online]. Available: https://www.buybitcoinworldwide.com/confirmations/. [Accessed 3 April 2019].

[11] M. Rosenfeld, "Analysis of hashrate-based double-spending," 13 December 2012. [Online]. Available: https://bitcoil.co.il/Doublespend.pdf. [Accessed 7 April 2019].

[12] "bitinfocharts.com," [Online]. Available: https://bitinfocharts.com/comparison/bitcoin-confirmationtime.html. [Accessed 27 March 2019].

[13] "tradeblock.com," [Online]. Available: https://tradeblock.com/bitcoin/historical/1d-f-blksize_per_tot-01071-tps-01071. [Accessed 27 March 2019].

[14] "Mini Validator List," [Online]. Available: https://minivalist.cinn.app/. [Accessed 4 April 2019].

[15] "bitinfocharts.com," [Online]. Available: https://bitinfocharts.com/comparison/bitcoin-transactionfees.html. [Accessed 29 March 2019].

[16] "bitinfocharts.com," [Online]. Available: https://bitinfocharts.com/comparison/transactionfees-xrp.html. [Accessed 6 April 2019].

[17] "nbcnews.com," MSNBC, [Online]. Available: https://www.nbcnews.com/tech/internet/bitcoin-loses-more-half-its-value-amid-crypto-crash-n844056. [Accessed 7 April 2019].

[18] "developers.ripple.com," Ripple, [Online]. Available: https://developers.ripple.com/transaction-cost.html. [Accessed 7 April 2019].

[19] "developers.ripple.com," Ripple, [Online]. Available: https://developers.ripple.com/technical-faq.html. [Accessed 11 April 2019].

[20] "bitinfocharts.com," [Online]. Available: https://bitinfocharts.com/comparison/bitcoin-hashrate.html. [Accessed 3 April 2019].

[21] "cia.gov," Central Intelligence Agency US, [Online]. Available: https://www.cia.gov/library/publications/the-world-factbook/rankorder/2233rank.html. [Accessed 3 April 2019].

[22] "economist.com," The Economist, [Online]. Available: https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy. [Accessed 3 April 2019].

[23] "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," 14 January 2019. [Online]. Available: https://lightning.network/lightning-network-paper.pdf. [Accessed 11 April 2019].

Appendix

Sites run by enthusiasts:
https://bitinfocharts.com
https://minivalist.cinn.app/
https://ledger.exposed/rich-stats
https://www.coingecko.com
https://coinmarketcap.com/
https://www.livecoinwatch.com/
https://bitcoin.org
Forums worth visiting:
www.xrpchat.com
https://www.reddit.com/r/CryptoCurrency/
https://www.reddit.com/r/ripple
https://www.reddit.com/r/bitcoin
https://github.com/bitcoin/bips
https://github.com/ripple